

ITAÚ UNIBANCO HOLDING S.A.

VERSÃO PARA DIVULGAÇÃO PÚBLICA

POLÍTICA CORPORATIVA DE SEGURANÇA DA INFORMAÇÃO E CYBER SECURITY

OBJETIVO

Estabelecer os princípios, diretrizes e atribuições relacionadas à segurança da informação, protegendo as informações da instituição, dos clientes e do público em geral, observando as melhores práticas de mercado e regulamentações aplicáveis.

PÚBLICO-ALVO

Colaboradores do Itaú Unibanco Holding e suas empresas controladas no Brasil e no exterior e entidades mantidas ou geridas pelo Conglomerado Itaú Unibanco.

INTRODUÇÃO

A informação é o principal ativo da instituição. Assim, o Itaú Unibanco Holding S.A define a estratégia de segurança da Informação e Cyber Security para proteger a integridade, disponibilidade e confidencialidade da informação.

Esta estratégia é baseada na detecção, prevenção, monitoramento e resposta à incidentes e fortalece a gestão do risco de segurança cibernética e a construção de um alicerce robusto para o futuro cada vez mais digital do Itaú Unibanco.

Para alcançarmos esse objetivo, utilizamos a estratégia de proteção de perímetro expandido. Esse conceito considera que a informação deve ser protegida independentemente de onde esteja, seja internamente, em uma coligada, em um serviço de cloud, em um prestador de serviço ou em uma unidade internacional, em todo o seu ciclo de vida, desde a coleta até o descarte.

PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

Nosso compromisso com o tratamento adequado das informações do Itaú Unibanco, clientes e público em geral está fundamentado nos seguintes princípios:

Confidencialidade: garantir que o acesso à informação seja obtido somente por pessoas autorizadas;

Disponibilidade: garantir que as pessoas autorizadas tenham acesso à informação sempre que necessário;

Integridade: garantir a exatidão e a completude da informação e dos métodos de seu processamento, bem como da transparência no trato com os públicos envolvidos.

DIRETRIZES

Os documentos de segurança da informação (política, regras e procedimentos) devem estar disponíveis em local acessível aos colaboradores e protegidos contra alterações.

A Política Corporativa de Segurança da Informação e Cyber Security é revisada anualmente pelo Itaú Unibanco com aplicação no Brasil e no exterior.

A inclusão de diretrizes ou exceções por requisito regulatório e a publicação nas unidades do exterior, serão identificadas pelo responsável por segurança da informação da unidade, que deverá formalizar e submeter de forma prévia a proposta de diretrizes ou exceções para aprovação pela Diretoria Cyber Security.

A adesão à essa Política e eventuais desvios, no Brasil e nas unidades no exterior, são reportados periodicamente pela Diretoria Cyber Security aos Comitê Executivo, Comitê de Auditoria e demais comitês de risco.

A informação deve ser utilizada de forma transparente, para as finalidades informadas ao cliente e de acordo com a legislação vigente, conforme descrito no documento específico e documento específico.

As diretrizes e eventuais exceções são complementadas em procedimentos com regras específicas que devem ser observadas.

Os princípios, diretrizes, processos e controles de Segurança da Informação e Cyber Security estabelecidos nesta Política aplicam-se integralmente ao ambiente computacional, incluindo os sistemas e infraestruturas que suportam a prestação de serviços de ativos virtuais e a comunicação eletrônica de dados na Rede do Sistema Financeiro Nacional (RSFN), em conformidade com a regulamentação vigente e com os padrões corporativos da instituição.

PROGRAMA DE CYBER SECURITY

O Programa de Cyber Security tem como objetivo monitorar, avaliar e analisar o desempenho e a conformidade dos processos relacionados à Segurança da Informação e à Cyber Security. Ele é fundamentado na gestão de riscos, utilizando a metodologia do Mapa de Riscos de Segurança, que permite uma avaliação estruturada do ambiente de controle.

Além disso, o programa é estruturado como um modelo interno de maturidade, com avaliações periódicas anuais, possibilitando o acompanhamento contínuo da evolução e da efetividade das práticas de segurança adotadas pela organização.

O programa é norteado pelos seguintes princípios:

Regulamentações vigentes;

Melhores práticas;

Cenários mundiais;

Análises de risco da própria instituição.

Conforme sua criticidade, as ações do programa dividem-se em:

Críticas: Consiste em correções emergenciais e imediatas para mitigar riscos iminentes;

Sustentação: Iniciativas de curto/médio prazo, para mitigação de risco no ambiente atual, mantendo o ambiente seguro, respeitando o apetite de risco da instituição e permitindo que ações de longo prazo/estruturantes possam ser realizadas;

Estruturantes: Iniciativas de médio/longo prazo que tratam a causa raiz dos riscos e que preparam o Itaú Unibanco para o futuro.

PROCESSOS DE SEGURANÇA DA INFORMAÇÃO

Para assegurar que as informações tratadas estejam adequadamente protegidas, o Itaú Unibanco adota os seguintes processos:

Gestão de Ativos

Entende-se por ativo, tudo aquilo que a instituição considerar como relevante para o negócio, desde ativos tecnológicos (p.ex. software e hardware) como não tecnológicos (p.ex. pessoas, processos e dependências físicas) desde que estejam relacionados à proteção da informação.

Os ativos tecnológicos, de acordo com sua criticidade, devem ser identificados, inventariados, mantidos atualizados, possuírem um proprietário, descartados de forma segura e serem protegidos contra acessos indevidos. A proteção pode ser, física (p.ex. salas com acesso controlado) e lógica (p.ex. configurações de blindagem ou hardening, patch management, autenticação, autorização e monitoramento).

Os ativos do Itaú Unibanco, dos clientes e do público em geral devem ser tratados de forma ética e sigilosa e de acordo com as leis vigentes e normas internas, promovendo o uso adequado e prevenindo exposição indevida das informações.

Classificação da Informação

As informações devem ser classificadas de acordo com a confidencialidade, conforme descrito nos documentos documento específico E documento específico para as Unidades Internacionais.

Para isso, devem ser consideradas as necessidades relacionadas ao negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações. De acordo com a classificação da confidencialidade devem ser estabelecidas as proteções necessárias durante todo o seu ciclo de vida.

O ciclo de vida da informação compreende: Geração, Manuseio, Armazenamento, Transporte e Descarte.

Gestão de Acessos

As concessões, revisões e exclusões de acesso devem utilizar as ferramentas e os processos corporativos do Itaú Unibanco.

Os acessos devem ser rastreáveis, a fim de permitir a identificação individual do colaborador ou prestador de serviço que tenha acessado ou alterado as informações, permitindo sua responsabilização.

A concessão de acessos deve obedecer ao critério de menor privilégio, no qual os usuários devem ter acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades e devidamente autorizados.

A segregação de funções deve permear todos os processos críticos, evitando que um único responsável possa executar e controlar o processo durante todo seu ciclo de vida.

A identificação de qualquer colaborador deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas.

A senha é uma informação confidencial, pessoal e intransferível, deve ser utilizada como assinatura eletrônica, sendo proibido seu compartilhamento.

Gestão de Riscos

Os riscos devem ser identificados por meio de processos estabelecidos para análise de ameaças, identificação de vulnerabilidades, análise de probabilidades e impactos sobre os ativos do Itaú Unibanco, para que sejam recomendadas as proteções adequadas. As recomendações são discutidas nos fóruns apropriados.

Produtos, processos e tecnologias devem ter a adequada gestão dos riscos de Segurança da Informação, para redução dos riscos à níveis aceitáveis, independentemente de estarem dentro da infraestrutura do Itaú Unibanco Holding, parceiros ou prestadores de serviços.

As tecnologias em uso pela instituição devem estar em versões suportadas pelos seus fabricantes e devidamente atualizadas, de acordo com os processos de gestão de patches. Eventuais exceções devem ser aprovadas na alçada competente ou possuir controles compensatórios.

Gestão de Riscos em Prestadores de Serviços e Parceiros

Os prestadores de serviços e parceiros contratados pelo Itaú Unibanco devem ser classificados considerando critérios, conforme documento específico e seus anexos.

De acordo com a classificação, o prestador de serviço ou parceiro passará por avaliação de risco, que pode incluir a validação in loco dos controles de Segurança da Informação, avaliação remota das evidências ou outras avaliações, além do acompanhamento de eventuais correções e melhorias implementadas pelos prestadores de serviços e parceiros.

Os prestadores de serviços e parceiros devem informar os incidentes relevantes (conforme definido no item 6.f deste documento), relacionados às informações do Itaú Unibanco armazenadas ou processadas por eles em cumprimento às determinações legais e regulamentares.

As diretrizes para contratação de serviços relevantes conforme definições regulamentares, estão descritas nos procedimentos documento específico e documento específico.

Tratamento de Incidentes de Segurança da Informação e Cyber Security

A área de Cyber Security monitora a segurança do ambiente tecnológico do Itaú Unibanco no Brasil, analisando os eventos e alertas para identificar possíveis incidentes.

Os incidentes que são identificados pelos alertas são classificados com relação ao impacto, de acordo com os critérios adotados pelo Itaú Unibanco. Para o seu grau de relevância serão considerados aspectos como impacto ao sistema financeiro e comprometimento de dados de clientes e do público em geral, conforme descrito no documento específico.

Todos os incidentes passam por um processo de avaliação, onde são registradas todas as informações pertinentes aos incidentes como causa, impacto, classificação e demais informações necessárias. Após avaliação, conforme governança descrita no documento específico, os incidentes classificados como relevantes com recomendação de comunicação, deverão ser comunicados ao Regulador e/ou ao titular dos dados, bem como ao Comitê de Auditoria (CAUD). Havendo o envolvimento de colaboradores internos, os casos serão reportados para atuação conjunta com a Inspecção.

Informações sobre incidentes que possam impactar outras instituições financeiras no Brasil, devem ser compartilhadas com as demais instituições, visando colaborar com a mitigação do risco conforme determinações legais e regulamentares.

No exterior, a gestão de incidentes de segurança da informação e cibernéticos é realizada por cada Unidade Internacional que deve reportá-los tempestivamente à Diretoria Cyber Security no Brasil.

A Diretoria Cyber Security elaborará relatórios anuais contendo os incidentes relevantes ocorridos no período, ações realizadas de prevenção e resposta aos incidentes e resultados dos testes de continuidade. Este relatório deverá ser apresentado ao Comitê de Risco, ao Comitê de Auditoria e ao Conselho de Administração, conforme determinações legais e regulamentares.

Visando aprimorar a capacidade de resposta a incidentes, o Itaú Unibanco realiza semestralmente testes de continuidade de negócios simulando cenários de incidentes críticos de Cyber Security, que podem comprometer a disponibilidade e/ou a confidencialidade das informações.

A fim de se antecipar às novas ameaças, o Itaú Unibanco mantém processos de inteligência sobre ameaças virtuais, além de participar ativamente de fóruns de cibersegurança da indústria e do governo, no Brasil e no exterior, para o fortalecimento das defesas.

Todo colaborador deve ser proativo e diligente na identificação, comunicação para a Diretoria Cyber Security e na mitigação dos riscos relacionados à segurança da informação.

Conscientização em Segurança da Informação e Cyber Security

O Itaú Unibanco promove a disseminação dos princípios e diretrizes de Segurança da Informação por meio de programas de conscientização e capacitação para fortalecer a cultura de Segurança da Informação e Cyber Security, fazendo parte do Programa de Integridade e Ética.

Periodicamente, são disponibilizadas campanhas de conscientização ou treinamentos que podem ser presenciais ou on-line, relacionados a confidencialidade, integridade e disponibilidade da informação. Estas campanhas são veiculadas através de e-mails, portal corporativo, e-learning, em mídias ou redes sociais aos colaboradores e clientes.

Governança com as Áreas de Negócio e Tecnologia

As iniciativas e projetos das áreas de negócio e tecnologia devem estar alinhadas com os princípios e diretrizes de segurança da informação.

Segurança Física do Ambiente

O processo de Segurança Física estabelece controles relacionados à concessão de acesso físico aos ambientes, de acordo com a criticidade das informações tratadas nestes ambientes, conforme descrito nos documentos documento específico e documento específico.

Segurança no Desenvolvimento de Sistemas de Aplicação

O processo de desenvolvimento de sistemas deve garantir a aderência aos documentos documento específico, documento específico para as Unidades Internacionais e às boas práticas de segurança da instituição.

A integração de sistemas de informação realizada por meio de interfaces eletrônicas deve ser projetada, implementada e mantida em conformidade com os requisitos de segurança da informação definidos pela instituição, garantindo controles adequados de acesso, proteção dos dados e rastreabilidade das operações.

Os ambientes produtivos devem ser segregados dos demais ambientes e com acesso somente via aplicação por usuários previamente autorizados ou por ferramentas homologadas.

Configuração Segura

O processo de configuração segura deve garantir a aderência a documento específico definida pela área de Arquitetura de Segurança da Informação, estabelecendo uma configuração segura dos sistemas adquiridos pela instituição de acordo com as boas práticas de Segurança.

Gravação de Logs

É obrigatória a gravação de logs ou trilhas de auditoria do ambiente computacional, para todas as plataformas, de forma a permitir identificar: quem fez o acesso, quando o acesso foi feito, o que foi acessado e como foi acessado.

Essas informações devem ser protegidas contra modificações e acessos não autorizados, conforme descrito no documento documento específico.

Proteção de perímetro

Para proteção da infraestrutura do Itaú Unibanco contra um ataque externo, utilizamos, no mínimo, ferramentas e controles contra: ataques de indisponibilidade (DDoS), Spam, Phishing, APT/Malware, invasão de dispositivos de rede e servidores, ataques a aplicação, além de processos de scan de vulnerabilidades externos e internos e testes de penetração.

Para mitigação do risco de vazamento de informações utilizamos ferramentas preventivas instaladas em dispositivos móveis, estações de trabalho e servidores, no serviço de correio eletrônico, no serviço de navegação WEB, no serviço de impressão, além do uso de criptografia para dados em repouso e em transporte.

Visando elevar a proteção, não é permitida a conexão física ou lógica à rede corporativa da instituição, por equipamentos particulares não gerenciados ou não homologados pelo Itaú Unibanco.

Proteção interna

Para proteção da infraestrutura do Itaú Unibanco contra ataques internos, utilizamos ferramenta de antimalware homologada contra ameaças cibernéticas. O antimalware é responsável pela detecção, proteção e mitigação dessas ameaças.

Governança com as Unidades Internacionais

As unidades internacionais devem possuir um responsável por segurança da informação, independente das áreas de negócio e tecnologia, que se reporta matricialmente à Diretoria Cyber Security.

Resiliência Cibernética

A Resiliência Cibernética é a capacidade de gerenciar e recuperar o ambiente diante de ataques cibernéticos, protegendo a integridade e a confidencialidade dos dados, sendo um dos princípios fundamentais do Programa de Resiliência Organizacional do Itaú Unibanco Holding S.A., conforme descrito no documento documento específico.

Propriedade Intelectual

A propriedade intelectual é a proteção que recai sobre bens imateriais, tais como: marcas, sinais distintivos, slogans publicitários, nomes de domínio, nomes empresariais, indicações geográficas, desenhos industriais, patentes de invenção e de modelo de utilidade, obras intelectuais (tais como obras

literárias, artísticas e científicas, base de dados, fotografias, desenhos, ilustrações, projetos de arquitetura, obras musicais, obras audiovisuais, textos e etc.), programas de computador e segredos empresariais (inclusive segredos de indústria e comércio).

Pertencem exclusivamente ao Itaú Unibanco todas e quaisquer invenções, criações, obras e aperfeiçoamentos que tenham sido ou venham a ser criados ou realizados pelo colaborador ao Itaú Unibanco, na qualidade de administrador, empregado e/ou estagiário, durante todo o prazo de vigência do mandato, contrato de trabalho ou contrato de estágio do colaborador. Quaisquer informações e conteúdos cuja propriedade intelectual pertença ao Itaú Unibanco, ou tenham sido por ele disponibilizado, inclusive informações e conteúdos que tenham sido obtidos, inferidos ou desenvolvidos pelo próprio colaborador em seu ambiente de trabalho ou utilizando recursos da instituição não devem ser utilizados para fins particulares, nem repassados a terceiros, sem autorização prévia e expressa do Itaú Unibanco.

É dever de todos os colaboradores zelar pela proteção da propriedade intelectual do Itaú Unibanco.

Declaração de Responsabilidade

Periodicamente os colaboradores do Itaú Unibanco devem aderir formalmente a um termo, comprometendo-se a agir de acordo com as políticas de Segurança da Informação.

Os contratos firmados com o Itaú Unibanco devem possuir cláusula que assegure a confidencialidade das informações e a obrigatoriedade de seguir as regulamentações vigentes, referentes ao tema de segurança da informação.

PAPÉIS E RESPONSABILIDADES

As políticas, estratégias e processos corporativos de Segurança da Informação são supervisionadas no Brasil e no exterior pela Diretoria Cyber Security e discutidos nos fóruns específicos de riscos das áreas e nas Comissões Executivas que tratam Risco Operacional ou Tecnologia.

Colaborador

Proteger as informações da organização e atuar de forma proativa e consciente para assegurar a integridade, confidencialidade e disponibilidade dos dados corporativos, em conformidade com as políticas de Segurança da Informação, são ações que constituem uma responsabilidade compartilhada por todos os colaboradores.

Cyber Security

A Diretoria Cyber Security compromete-se com a melhoria contínua de seus sistemas, processos e práticas, visando garantir a integridade, disponibilidade e confidencialidade das informações. Para isso, são adotadas as seguintes diretrizes:

Aprimorar continuamente a qualidade e efetividade dos processos de segurança da informação, com foco na proteção dos ativos informacionais e na mitigação de riscos ao negócio;

Proteger as informações contra ameaças internas e externas, assegurando a continuidade das operações e a resiliência organizacional;

Estabelecer, implementar, operar, monitorar e revisar o Sistema de Gestão Integrado (SGI) promovendo sua melhoria contínua com base em indicadores, auditorias e lições aprendidas;

Definir e formalizar objetivos, controles e as estratégias de governança de segurança da informação, em conjunto com o Comitê Executivo de Segurança da Informação, garantindo alinhamento com as diretrizes corporativas;

Coordenar e acompanhar ações estratégicas, envolvendo as áreas responsáveis, para o atingimento dos objetivos definidos pelos comitês;

Promover e disseminar uma cultura organizacional voltada à segurança da informação, incentivando comportamentos seguros e conscientes;

Propor investimentos estratégicos que viabilizem o cumprimento dos objetivos da política de segurança da informação;

Estabelecer políticas e padrões de segurança da informação aplicáveis aos processos, produtos e tecnologias, com foco na consistência e conformidade;

Definir padrões mínimos de segurança para as Unidades Internacionais, Empresas controladas no Brasil e no exterior, e Entidades mantidas ou geridas pelo Conglomerado Itaú Unibanco, assegurando alinhamento com os objetivos de segurança da informação definidos pela Holding;

Definir, monitorar, gerir e reportar as métricas de apetite de risco sob responsabilidade da Segurança da Informação, relacionadas ao nível executivo (Comitê Executivo - CE), assegurando alinhamento com as diretrizes corporativas e suporte à tomada de decisão estratégica.

Auditoria Interna

Os papéis e responsabilidades da Auditoria Interna estão descritos no documento específico.

Risco Operacional

Os papéis e responsabilidades de Risco Operacional estão descritos no documento específico.

Unidades Internacionais

Atuar proativamente na identificação, prevenção e correção dos riscos e reportar periodicamente à Diretoria Cyber Security.

Empresas e Entidades do Conglomerado

Empresas do conglomerado controladas no Brasil e no exterior e entidades mantidas ou geridas pelo Conglomerado Itaú Unibanco devem avaliar as diretrizes e requisitos estabelecidos nesta política e em seu anexo, reportando periodicamente à Diretoria Cyber Security os riscos identificados, adequando seus procedimentos de segurança internos conforme seu segmento de negócio e apetite de riscos. Estas empresas devem ser classificadas e ter modelo de governança baseado na avaliação de riscos, que considera os seguintes aspectos: Impacto na imagem da Holding, Modelo de Arquitetura e Conectividade com a Holding, e Volume de dados sensíveis armazenados. Este modelo de governança pode variar entre avaliação e acompanhamento direto de aderência aos controles definidos ou seguindo declaração de aderência a ser realizado pela própria empresa.

Comitê Executivo de Segurança da Informação

Aprovar a estratégia, objetivos, orçamento e ações necessárias para a mitigação dos riscos dos processos de segurança da informação.

Comitê de Auditoria – CAUD

Supervisionar a estratégia de gestão dos riscos, seus respectivos processos e controles internos, bem como acompanhar os projetos de segurança da informação do Conglomerado Itaú Unibanco.

Área de Tecnologia

Manter o parque tecnológico disponível e atualizado com os padrões de segurança implementados, dentro dos prazos compatíveis com os níveis de riscos.

Área de Negócio

Proteger as informações do Itaú Unibanco sob sua responsabilidade.

SANÇÕES DISCIPLINARES

As violações a esta política estão sujeitas às sanções disciplinares previstas no documento específico e no documento específico, bem como nas normas internas das empresas do Itaú Unibanco e na legislação vigente onde as empresas estiverem localizadas.

10.2. Documento de Acesso Público

O documento de acesso público pode ser encontrado no site de Relações com Investidores:

<https://www.itaú.com.br/relacoes-com-investidores/>

10.3. Frameworks e Regulamentações

Resolução CMN nº 4.893/2021 do Banco Central;

Resolução BCB nº 85/2021 do Banco Central;

Lei Geral de Proteção de Dados Pessoais nº 13.709/2018 (LGPD);

Resolução CD/ANPD nº 15/2024;

Resolução CVM nº 35/2021;

Resolução Conjunta BACEN nº 1/2020 (Open Finance);

Circular SUSEP nº 638/2021;

Resolução CNSP nº 415/2021 (Open Insurance);

Resolução Normativa ANEEL nº 964/2021;

Securities and Exchange Commission (SEC) - Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure;

E demais regulamentações e leis relacionadas ao tema.

ABNT NBR ISO/IEC 27001:2022 – Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação - Requisitos

ABNT NBR ISO/IEC 27701:2019 – Técnicas de segurança – Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação – Requisitos e diretrizes.

GLOSSÁRIO

APT (Advanced Persistent Threat): ataques avançados persistentes.

Cyber Security: é o termo que designa o conjunto de meios e tecnologias empregadas na defesa dos sistemas de informação, infraestrutura, redes de computadores e/ou dispositivos pessoais, com o objetivo de prevenir danos, roubo, intrusão, alterações ou destruição de informações.

Dano Relevante: Ação que possa causar impacto à privacidade do indivíduo, podendo ocasionar risco elevado à sua integridade física ou moral.

Parque tecnológico: conjunto de ativos de infraestrutura e sistemas de tecnologia.

Segregação de funções: consiste na separação das atividades entre áreas e pessoas potencialmente conflitantes ou que possuem informações privilegiadas, na qual, o colaborador não pode exercer mais que uma função nos processos de autorização, aprovação, execução, controle e contabilização.

Aprovado pelo Conselho de Administração em setembro de 2026.